DRN-3263416

The complaint

Mr P complains about how PayPal (Europe) Sarl et Cie SCA implemented new rules on authenticating customers. He says what they did meant he lost access to his PayPal account.

What happened

Mr P says that when PayPal made changes to the way a customer accesses their account, he lost access. The changes meant he could no longer access his account by simply using his email address and entering his password; he was required to also confirm a telephone number linked to his account by receiving a code to it.

Although Mr P does use a mobile phone and had previously linked that number to his PayPal account, he was finding that the code was expiring before it was received. He spoke with his mobile phone operator who told him PayPal's SMS messages needed a long processing time.

When he contacted PayPal in October 2020 via 'chat' services and social media seeking to resolve the problem, they were unable to add a landline number to his account for him to use for authenticating instead. Considering this, he suggested that PayPal either; send a time limited code to him by email, adopt a second password, or allow him to bypass this layer of authentication until the issue with the SMS messages had been resolved. As PayPal didn't adopt these suggestions or offer another resolution, Mr P says he was prevented from retrieving the funds in his account (approximately £100).

PayPal told Mr P they could see no reason why the SMS messages weren't reaching him in time. They suggested he call to speak with an agent, but he said he'd already tried that a number of times and couldn't get through. He said when he called he repeatedly received a message directing him back to the website. As he didn't feel he was getting anywhere with PayPal, Mr P complained.

PayPal responded to Mr P's complaint on 14 January 2021. They said:

- They'd made changes to the way customers access their accounts in response to the Payment Services Directive (PSD2) which brought in a requirement for payment service providers to implement two-factor or strong customer authentication (SCA);
- Mr P had attempted to login to his account on 21 and 23 October 2020, however, it was stopped by the security system and he was required to complete SCA;
- As they'll sometimes require Mr P to receive and enter a one-time passcode (OTP) to a phone number registered with them, it's important his phone details are kept up to date; and
- They didn't accept Mr P's complaint because they'd sent OTPs to his mobile number in October 2020 and couldn't identify any issues that would have caused a delay in him receiving those messages.

Mr P remained dissatisfied as PayPal hadn't offered him any alternative way of accessing his account.

What PayPal told us

PayPal told us they understand Mr P to be "*not willing*" to complete the SCA process but they have no choice but to implement the requirements of PSD2. They said SCA is more likely to be triggered if a consumer attempts to access their account via a virtual private network (VPN), so Mr P can reduce the number of times he's asked to complete SCA if he avoids using a VPN.

Our investigator's view

Our investigator upheld Mr P's complaint. He said that whilst PayPal hadn't acted unfairly by introducing SCA, they should have done more to help Mr P when he told them he was struggling to receive the authentication codes or OTPs to his mobile phone number. The investigator cited the Financial Conduct Authority's (FCA's) guidance on the implementation of SCA which sets out their expectation that payment service providers (PSPs), like PayPal, will develop SCA solutions that work for all groups of customers.

The investigator said that PayPal hadn't offered Mr P any viable alternatives for accessing his account beyond telling him that he could reduce the number of times he's asked to complete the SCA step if he avoids using VPNs, and he didn't think this was fair.

To put things right the investigator said PayPal should pay Mr P £100 compensation for the distress and inconvenience caused by their poor service, and offer Mr P another method to authenticate which doesn't rely on his mobile phone.

Responses to the view

Mr P asked the investigator to amend his recommendations to make it clearer that PayPal ought to pay him £100 compensation and return to him the funds still held in his PayPal account.

PayPal didn't accept what the investigator had said. They said they'd already offered Mr P "*multiple viable alternatives*" but Mr P had refused to use these options to access his account and funds. PayPal directed us to a page of their website which explains SCA and includes the following:

> "*If we need to ask you for a one-time passcode we can send it by SMS to your mobile phone number or via phone call to your landline, so your payment or login won't be delayed*."

The page goes on to explain that PayPal also use device recognition, so an OTP isn't always necessary:

> "*Most times, we'll be able to verify your identity using the PayPal password you've typed and the device you're using (if it's one of your usual devices). So, you may continue to login to your PayPal account or pay with PayPal as usual, using your email address and your PayPal password*."

The page also explains that customers can complete SCA: via the PayPal app; by entering an OTP sent to a phone number; or by generating an OTP with a third-party authenticator app.

Mr P maintained that PayPal hadn't offered him an alternative means of verifying his identity and had only offered to send the OTPs to his mobile phone, which wasn't working for him.

As no agreement could be reached, the complaint was passed to me to decide.

My provisional decision

I issued a provisional decision on 7 December 2021. I began by setting out the considerations I thought relevant to my decision. I wrote:

> "*I'm required to determine this complaint by reference to what I consider to be fair and reasonable in all the circumstances of the case. When considering what is fair and reasonable, I am required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.*
>
> *So, I'll start by setting out what I have identified as the relevant considerations to deciding what is fair and reasonable in this case.*
>
> *The Payment Services Regulations 2017 (PSRs) Reg. 100, which came into force on 14 September 2019, says that a payment service provider (PSP) must apply "strong customer authentication" where a "payment service user" accesses its payment account online, initiates an electronic payment transaction; or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.*
>
> *SCA is defined in the PSRs. It means:*
>
> > *"authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, and designed in such a way as to protect the confidentiality of the authentication data, with the elements falling into two or more of the following categories—*
> >
> > > *(a) something known only by the payment service user ("knowledge");*
> > > *(b) something held only by the payment service user ("possession");*
> > > *(c) something inherent to the payment service user ("inherence");"*
>
> *Another relevant consideration is the SCA implementation guidance issued by the Financial Conduct Authority (FCA) in its document "Payment Service and Electronic Money – Our Approach" (June 2019) and related statements.*
>
> *The FCA's guidance document says:*
>
> > *"… it may be necessary for a PSP to provide different methods of authentication, to comply with their obligation to apply strong customer authentication in line with [PSD2]. For example, not all payment service users will possess a mobile phone or smart phone and payments may be made in areas without mobile phone reception. PSPs **must** provide a viable means to strongly authenticate customers in these situations." (my emphasis)*
>
> *In its statement of expectations published in September 2019, the FCA also said:*
>
> > *"We expect firms to develop SCA solutions that work for all groups of consumers. This means that you may need to provide several different methods of authentication for your customers. This includes methods that*

don't rely on mobile phones, to cater for consumers who don't have, or won't want to use, a mobile phone."

What I've provisionally decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so I've reached the same outcome as our investigator and for broadly the same reasons.

I think the above relevant considerations mean that PayPal were required to implement SCA, and so I don't think they've acted unfairly by doing that. The intention of the new SCA rules is to protect both businesses and consumers from fraudulent activity and that is, of course, to be welcomed. The FCA's guidance also makes it clear that processes reliant on mobile phone ownership won't be suitable for all customers and PSPs must provide viable alternatives.

PayPal have shown that they do offer a range of SCA compliant verification options. But I've seen no evidence that when Mr P let PayPal know he was having difficulty receiving their OTPs to his mobile phone, they helped him towards using one of the alternatives they offer.

I've read through the electronic exchanges PayPal had with Mr P from October to December 2020 and I can see that he was seeking to update his account so that his landline telephone number could be used for SCA. But I don't think PayPal did enough to help him achieve that.

PayPal have suggested that Mr P is not willing to complete the extra authentication step that SCA involves. I don't agree that's the case. Indeed, Mr P made some suggestions for an alternative extra step when he was corresponding with PayPal. So, I think it's more likely than not he'd have accepted authenticating using his landline if PayPal had made that solution possible.

Because of his frustrating exchanges with PayPal Mr P abandoned further attempts to access his PayPal account. If he'd persisted in trying, I accept it's possible that at some point between October 2020 and now he'd have found whatever was causing PayPal's SMS messages to be delayed has resolved. However, in the circumstances I don't think it was incumbent on him to keep trying.

By not helping Mr P to access his account using another of their options for authentication, I think PayPal caused Mr P distress and inconvenience as he was unable to use his account or remove his funds (approximately, £100). So, overall, I don't think PayPal treated Mr P fairly and reasonably. And I think it's right that PayPal pay him £100 compensation and, moving forward, enable Mr P to complete the SCA process without reliance on his mobile phone if he is still finding the OTPs have expired before receipt."

Responses to the provisional decision

PayPal agreed to pay Mr P £100 and advised that if he was still having trouble receiving OTPs to his mobile phone, he could try using an authenticator app which can be downloaded to a desktop personal computer or smart phone and generates a passcode which can be used for two factor authentication (SCA). They also told our service that there

is currently an issue with authenticating using a landline telephone number, and they don't have a clear timeframe for when that will be resolved.

Mr P explained he's never used a VPN and said he couldn't receive PayPal's text messages because his network provider interpreted them as "*spam*". He explained, "*PayPal have neither disabled the SCA option nor introduced an alternative means of accessing the account!*". He also said he has no desire to continue using PayPal's services.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Having done so, I see no reason to depart from what I said in my provisional decision. I remain of the view that whilst PayPal did nothing wrong by implementing SCA - an important regulatory measure designed to protect both PayPal and customers from fraud - PayPal failed to help Mr P access his account using another of their options for strong customer authentication (landline or authenticator app) when it became clear OTP to mobile wasn't working.

Mr P has told me that he no longer wants to be PayPal's customer because of his poor experience of their service. So, although I would have directed PayPal to help Mr P to complete the SCA process using one of their available alternative options to mobile phone if he still couldn't successfully receive OTPs to his mobile phone, I don't think I now need to make any direction about what authentication options PayPal should offer him going forwards. However, they should still, if he wishes to end his relationship with them, assist him with completing authentication so that he may withdraw any remaining balance he has in his PayPal account.

Putting things right

Ways of strongly authenticating customers which don't rely on the payment service user having a mobile phone or mobile device do exist and the relevant guidance says alternatives should be offered. So, I think it was unfair and unreasonable of PayPal not to help Mr P towards one of the alternatives they offer when he was struggling to receive OTPs to his mobile phone. To compensate him for the distress and inconvenience caused by this poor service I direct PayPal, if they've not already done so, to pay Mr P £100.

PayPal should also assist Mr P with completing authentication using his mobile phone or, if he's still having difficulty receiving OTPs by SMS, using an authenticator app, so that he may withdraw any remaining balance he has in his PayPal account.

My final decision

My final decision is that I uphold Mr P's complaint. PayPal (Europe) Sarl et Cie SCA should put things right in the way I've set out in the 'Putting things right – what PayPal needs to do' section of this decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr P to accept or reject my decision before 5 May 2022.

Beth Wilcox
Ombudsman